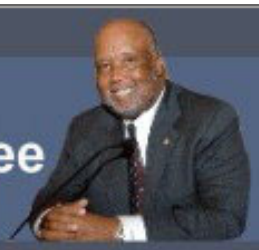
NEWS ALERT

U.S. HOUSE OF REPRESENTATIVES

Homeland Security Committee

Rep. Bennie G. Thompson, Ranking Member



FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson

H.R. 3696, the "National Cyber Security and Critical Infrastructure Protection Act"

February 5, 2014 (Washington) – Today, Committee on Homeland Security Ranking Member Bennie G. Thompson (D-MS) delivered the following prepared remarks for the full Committee markup of H.R. 3696, the "National Cyber Security and Critical Infrastructure Protection Act":

"I am pleased to be here today and to be an original cosponsor of H.R. 3696, the "National Cyber Security and Critical Infrastructure Protection Act." Today's mark-up represents a milestone for the Committee and this Congress.

After years of Congressional deadlock over cybersecurity, we have come together to provide the Department of Homeland Security with the authority and resources it needs to carry out its dual role as the lead Federal agency for protecting Federal civilian networks and the lead for partnering with our Nation's critical infrastructure for cybersecurity.

When it comes to protecting critical infrastructure, the bill takes a multi-faceted approach. Not only does it authorize information sharing mechanisms that are essential to ensuring that owners and operators can identify, contain, and mitigate wide-scale threats, it also authorizes the National Cybersecurity and Communications Integration Center and the so-called "cyber fly-away teams" that provide on-site technical assistance.

We have all heard the stories about massive cyber-crime, Internet fraud, and database thefts. In recent years, cyber crime has become so prevalent that companies have begun to factor it into their financial planning as "a cost of doing-business." Sharing cyber information will not create a threat-free environment, but we must encourage business and government to work together to do more. The information sharing provisions in this bill do just that.

Another strength of the bill is that it builds upon President Obama's Cybersecurity Executive Order, which, to date, represented the most significant advancement in efforts to bolster the level of cybersecurity within critical infrastructure. Executive Order 13636 set in motion the development of the Cyber Framework by the National Institute of Standards and Technology that is expected to be released later this month. The publication of the Framework has the potential to fundamentally alter how business decisions about network security get made.

When it comes to protecting Federal civilian networks, the bill, for the first time, would place, in law, DHS' roles, responsibilities, and authorities. Since the Bush Administration, the Department has been delegated responsibility for managing Federal efforts to secure, protect, and ensure the resiliency of Federal civilian networks. Today, DHS runs the government's continuous diagnostic program – EINSTEIN – and is charged with overseeing compliance of all Federal network security policies and procedures. However, if you look at the U.S. Code, you would not know it. H.R. 3696 would remedy that situation and, in the process, strengthen the Department's hand when dealing with other Federal agencies.

To execute its dual cyber mission, the Department must have a capable and stable workforce. The challenges of identifying, hiring, training, and retaining this workforce are complex. It is not simply a matter of money. To her credit, the Ranking Member of the Cybersecurity Subcommittee, Ms. Clarke, recognized this reality and authored comprehensive legislation that tackles these challenges. I am pleased that her bill - the "Homeland Security Cybersecurity Boots-On-The-Ground Act" - was accepted by her Cybersecurity Subcommittee colleagues, most especially, Chairman Meehan, and is part of the legislation we are considering today. It will help assure that DHS has the staffing resources necessary to undertake the full range of responsibilities under this Act.

I would be remiss if I did not express my appreciation for your willingness to set aside language that

Ranking Member Clarke, myself, Members of the Committee and the privacy and civil liberties community cautioned would produce unintended consequences. We are here today with a comprehensive, bipartisan bill because of our shared desire to legislate responsibly. When I learned that the ACLU, in its letter to the Committee, called the bill "both pro-security and pro-privacy," I took it as a positive signal.

I do not want to get ahead of myself and take a victory lap just yet. There are a few crucial stops along the way to H.R. 3696 becoming law but after today's mark-up, it will be one major step closer.

Before I yield back, I would note that today Democrats plan to offer a number of amendments that seek to make further improvements to the bill. I have reviewed the pre-filed amendments by the Democratic Members and would like to express, for the record, my support for them. In particular, there are a couple of anticipated amendments that seek to bolster transparency which warrant consideration."

# # #

FOR MORE INFORMATION: Please contact Adam Comis at (202) 225-9978

United States House of Representatives
Committee on Homeland Security
H2-117, Ford House Office Building, Washington, D.C. 20515
Phone: (202) 226-2616 | Fax: (202) 226-4499
http://chsdemocrats.house.gov